Higher Quality, Better Service!

KillTest

50% OFF
Coupon:off50

CYBERARK DEFENDER Exam

PAM-DEF Questions V11.02

CyberArk Defender

Topics - CyberArk Defender – PAM

1.If a user is a member of more than one group that has authorizations on a safe, by default that user is granted_____.
A. the vault will not allow this situation to occur.
B. only those permissions that exist on the group added to the safe first.
C. only those permissions that exist in all groups to which the user belongs.
D. the cumulative permissions of all groups to which that user belongs.
Answer: D
Explanation:
When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user's permissions to only those of the group added to the safe first.
Reference: [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2: Safe Permissions, Slide 8: Cumulative Permissions
[Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

2.It is possible to control the hours of the day during which a user may log into the vault.
A. TRUE
B. FALSE
Answer: A
Explanation:
It is possible to control the hours of the day during which a user may log into the vault by using the Time Restrictions feature. This feature allows administrators to define the days and times that users can access the vault. Users who try to log in outside the permitted hours will be denied access and receive a message informing them of the restriction. Time restrictions can be applied to individual users or groups of users.
Reference: [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.3: User Management,
Slide 7: Time Restrictions
[Defender PAM Sample Items Study Guide], Question 2: Time Restrictions
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 4: Managing Users and Groups, Section: Time Restrictions

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

3.VAULT authorizations may be granted to_____.
A. Vault Users
B. Vault Groups
C. LDAP Users
D. LDAP Groups
Answer: AC
Explanation:
Vault Authorizations
• Can be assigned only to users (not groups).
• Cannot be inherited via group membership.
• Defined only via the Private Ark Client. Safe Auth
• Assigned to users and/or groups.
• Can be inherited via group membership.
• Can be defined in the Private Ark Client or PVWA

4.What is the purpose of the Interval setting in a CPM policy?
A. To control how often the CPM looks for System Initiated CPM work.
B. To control how often the CPM looks for User Initiated CPM work.
C. To control how long the CPM rests between password changes.
D. To control the maximum amount of time the CPM will wait for a password change to complete.
Answer: A
Explanation:
The Interval setting in a CPM policy is used to control how often the CPM looks for System Initiated CPM work, such as password changes, verifications, and reconciliations. The Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the required actions. For example, if the Interval is set to 60, the CPM will check the accounts every hour and change, verify, or reconcile the passwords according to the policy settings. The Interval setting does not affect User Initiated CPM work, such as manual password changes or retrievals, which are performed immediately upon request. The Interval setting also does not control how long the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe.
Reference: [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide
9: CPM Policy Settings
[Defender PAM Sample Items Study Guide], Question 4: CPM Policy Settings
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Settings, Subsection: Interval

5.All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group Operations Staff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of Operations Managers never need to be able to use the show, copy or connect buttons themselves.
Which safe permission do you need to grant Operations Staff? Check all that apply.
A. Use Accounts
B. Retrieve Accounts
C. Authorize Password Requests
D. Access Safe without Authorization
Answer: A, B
Explanation:
To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password
Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval.
Reference: [Defender PAM Sample Items Study Guide], page 10, question 5
[CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1
[CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

6.What is the purpose of the Immediate Interval setting in a CPM policy?
A. To control how often the CPM looks for System Initiated CPM work.
B. To control how often the CPM looks for User Initiated CPM work.
C. To control how often the CPM rests between password changes.
D. To Control the maximum amount of time the CPM will wait for a password change to complete.
Answer: B
Explanation:
The Immediate Interval setting in a CPM policy is used to control how often the CPM looks for User Initiated CPM work, such as manual password changes, retrievals, or

requests. The Immediate Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the actions that were initiated by the users. For example, if the Immediate Interval is set to 2, the CPM will check the accounts every 2 minutes and change, retrieve, or authorize the passwords according to the user requests. The Immediate Interval setting does not affect System Initiated CPM work, such as password changes, verifications, or reconciliations that are triggered by the policy settings, such as Expiration Period or One Time Password. These actions are controlled by the Interval setting in the CPM policy. The Immediate Interval setting also does not control how often the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe.
Reference: [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide
9: CPM Policy Settings
[Defender PAM Sample Items Study Guide], Question 6: CPM Policy Settings
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Immediate Interval

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

7.Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.
A. PAR Agent
B. PrivateArk Server Central Administration
C. Edit DBParm.ini in a text editor
D. Setup.exe
Answer: A, B
Explanation:
To change debugging levels on the vault without having to restart the vault, you can use the following utilities:
PAR Agent: This is a utility that runs on the vault server and allows you to change the debug level of the vault by editing the PARAgent.ini file. You can set the EnableTrace parameter to yes and specify the debug level in the DebugLevel parameter. The changes will take effect immediately without restarting the vault. The log file is located in the PARAgent.log file1.
PrivateArk Server Central Administration: This is a graphical user interface that runs on the vault server and allows you to change the debug level of the vault by selecting the vault server and clicking the Debug button. You can choose the debug level from a list of predefined options or enter a custom value. The changes will take effect immediately without restarting the vault. The log files are located in the Trace.dX files, where X is a number from 0 to 42.
You cannot use the following utilities to change debugging levels on the vault without

having to restart the vault:
Edit DBParm.ini in a text editor: This is a configuration file that stores the vault parameters, such as the database name, port, and password. Editing this file does not affect the debug level of the vault, and requires restarting the vault for the changes to take effect3.
Setup.exe: This is an installation program that runs on the vault server and allows you to install, upgrade, or uninstall the vault. It does not allow you to change the debug level of the vault, and requires restarting the vault for any changes to take effect4.
Reference: 1: Configure Debug Levels, Vault section, PARAgent subsection
2: Configure Debug Levels, Vault section, PrivateArk Server Central Administration subsection
3: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault,
Section: Configuring the Vault, Subsection: DBParm.ini
4: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault,
Section: Installing the Vault

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

8.A Logon Account can be specified in the Master Policy.
A. TRUE
B. FALSE
Answer: B
Explanation:
A Logon Account cannot be specified in the Master Policy. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. A Logon Account is a technical setting that defines the account that the CPM uses to log on to a target system and perform password management tasks, such as changing, verifying, or reconciling passwords2. A Logon Account can be specified in the Platform Management settings, which are configured by the IT administrator for each platform2. The Platform Management settings are independent of the Master Policy and can be customized according to the organization's
environment and security policies1.
Reference: The Master Policy
[Platform Management]

9.For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.

A. Create an exception to the Master Policy to exclude the group from the workflow process.
B. Edith the master policy rule and modify the advanced' Access safe without approval' rule to include the group.
C. On the safe in which the account is stored grant the group the' Access safe without audit' authorization.
D. On the safe in which the account is stored grant the group the' Access safe without confirmation' authorization.
Answer: D
Explanation:
Dual Control is a feature that requires the approval of another user before accessing a password. It is based on a Master Policy rule that applies to all accounts attached to platforms that have this rule enabled. However, there may be situations where a group of users needs to access a password without approval, such as in an emergency or for troubleshooting purposes. In this case, an exception can be made by granting the group the 'Access safe without confirmation' authorization on the safe in which the account is stored. This authorization bypasses the Dual Control workflow and allows the group to retrieve the password without waiting for approval. However, the password retrieval will still be audited and recorded in the Vault.

10.As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.
A. TRUE
B. FALSE
Answer: B
Explanation:
Being a member of the Vault Admins group does not automatically grant you any permission on any safe that you have access to. The Vault Admins group is a predefined group that is created during the installation or upgrade of the vault. This group has the Vault Admin authorization, which allows its members to perform administrative tasks on the vault, such as managing users, groups, platforms, policies, and safes1. However, this authorization does not include any safe member authorizations, such as View, Retrieve, Use, or Manage Safe2. Therefore, to grant any permission on a safe, you need to be added as a safe member with the appropriate authorizations, either directly or through another group. The Vault Admins group can be added to safes with all safe member authorizations, but this is not done automatically for all safes. By default, this group is only added to a number of system safes, such as the Password Manager Safe, the PVWAConfig Safe, and the Notification Methods Safe3. For other safes, the Vault Admins group can be added manually by the safe owner or another user with the Manage Safe authorization4.
Reference: 1: Predefined users and groups, Predefined groups subsection
2: [CyberArk Privileged Access Security Implementation Guide], Chapter 3: Managing

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Safes, Section:
Safe Authorizations, Table 2-1: Safe Authorizations
3: What default groups can be automatically added to Safes when they are created?
4: [CyberArk Privileged Access Security Administration Guide], Chapter 3: Managing Safes, Section:
Adding Safe Members

11.Which report provides a list of account stored in the vault.
A. Privileged Accounts Inventory
B. Privileged Accounts Compliance Status
C. Entitlement Report
D. Active Log
Answer: A
Explanation:
The report that provides a list of accounts stored in the vault is the Privileged Accounts Inventory report. This report can be generated in the Reports page in the PVWA by users who belong to the group that is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page1. The Privileged Accounts Inventory report contains information such as the safe, folder, name, platform ID, username, address, group, last accessed date, last accessed by, last modified date, last modified by, verification date, checkout date, checked out by, age, change failure, verification failure, master pass folder, master pass name, disabled by, and disabled reason of each account stored in the vault2.
Reference: 1: Reports in PVWA
2: Users List Report

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

12.When on-boarding account using Accounts Feed, Which of the following is true?
A. You must specify an existing Safe where are account will be stored when it is on boarded to the Vault
B. You can specify the name of a new sale that will be created where the account will be stored when it is on-boarded to the Vault.
C. You can specify the name of a new Platform that will be created and associated with the account
D. Any account that is on boarded can be automatically reconciled regardless of the platform it is associated with.
Answer: B
Explanation:
When on-boarding accounts using Accounts Feed, you can either select an existing safe or create a new one to store the accounts. You can also specify the platform, policy, and owner for each account. However, you cannot create a new platform using

Accounts Feed, and not all platforms support automatic reconciliation.
Reference: Accounts Feed - CyberArk
CyberArk University
[Defender-PAM Sample Items Study Guide]

13.Target account platforms can be restricted to accounts that are stored m specific Safes using the Allowed Safes property.
A. TRUE
B. FALSE
Answer: A
Explanation:
Target account platforms can be restricted to accounts that are stored in specific Safes using the Allowed Safes property. This property is a parameter that can be configured in the Platform Management settings for each platform. The Allowed Safes property specifies the name or names of the Safes where the platform can be applied. The default value is .*, which means that the platform can be used in any Safe. However, if you want to limit the platform to certain Safes, you can enter the name or names of the Safes, separated by a pipe (|) character. For example, if you want to restrict the platform to Safes called WindowsPasswords and LinuxPasswords, you can enter AllowedSafes=(WindowsPasswords)|(LinuxPasswords). This feature is useful for preventing unauthorized users from accessing passwords, especially if you implement the reconciliation functionality. It also helps the CPM to focus its search operations on specific Safes, instead of scanning all Safes it can see in the Vault1.
Reference: 1: Limit Platforms to Specific Safes

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

14.Which one the following reports is NOT generated by using the PVWA?
A. Accounts Inventory
B. Application Inventory
C. Sales List
D. Convince Status
Answer: C
Explanation:
The PVWA can generate various reports on the privileged accounts and applications in the system, based on different filters and criteria. However, the Safes List report is not one of them. The Safes List report is generated by using the PrivateArk Client, and it provides a list of Safes and their properties according to location.
Reference: Defender-PAM Study Guide, Reports and Audits

15.PSM captures a record of each command that was executed in Unix.
A. TRIE

B. FALSE
Answer: A
Explanation:
PSM captures a record of each command that was executed in Unix by using the SSH text recorder. This is a feature that enables PSM to record all the keystrokes that are typed during privileged sessions on SSH connections, including Unix systems. The SSH text recorder can be configured in the Platform Management settings for each platform that uses the SSH protocol. The text recordings are stored and protected in the Vault server and are accessible to authorized auditors. The text recordings can also be used for auditing and compliance purposes, as they provide a detailed trace of the actions performed by the users on the target systems1.
Reference: 1: Introduction to PSM for SSH, How it works subsection, Text recordings paragraph

16.Platform settings are applied to _____.
A. The entire vault.
B. Network Areas
C. Safes
D. Individual Accounts
Answer: D
Explanation:
Platform settings are applied to individual accounts. A platform is a set of parameters that defines how the Vault manages the passwords of accounts that belong to a certain operating system or application. Each account in the Vault is attached to a platform that determines how the account password is changed, verified, reconciled, and accessed. Platform settings can be customized to meet the specific requirements of each account type. For example, you can define the password complexity, rotation frequency, verification method, and access policy for each platform.
Reference: [Defender PAM Sample Items Study Guide], page 15; [CyberArk Privileged Access Security Documentation], Platforms Overview.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

17.Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.
A. TRUE
B. FALSE
Answer: B
Explanation:
Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The ‘Access Safe without confirmation’ safe permission allows

users to access accounts without confirmation from authorized users, even if the Master Policy or an exception enforces Dual Control1. This means that users who have this permission can bypass the workflow process and access the account password or connect to the target system immediately. This permission can be granted to users or groups on a safe level by the safe owner or another user with the Manage Safe authorization2.
Reference: 1: Dual Control, Advanced Settings subsection
2: CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section:
Safe Authorizations, Table 2-1: Safe Authorizations

18.What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?
A. Min Validity Period
B. Interval
C. Immediate Interval
D. Timeout
Answer: A
Explanation:
The name of the Platform parameter that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy is Min Validity Period. This parameter defines the number of minutes to wait from the last retrieval of the account until it is replaced. This gives the user a minimum period to be able to use the password before it is changed by the CPM. The Min Validity Period parameter can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 60 minutes, but it can be modified according to the organization's security policy1. The Min Validity Period parameter is also used to release exclusive accounts automatically1.
Reference: 1: Privileged Account Management, Min Validity Period subsection

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

19.It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.
A. TRUE
B. FALSE
Answer: A
Explanation:
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection. Auto-detection is a feature that enables the CPM to automatically discover and onboard accounts on target systems that are associated with a specific platform. Auto-detection can be configured in the Platform Management settings for each platform that supports this functionality. However, auto-detection has some

limitations, such as requiring the CPM to have access to the target system, not supporting all platforms, and not providing comprehensive information about the accounts and their security risks1. DNA, on the other hand, is a standalone scanning tool that can discover and audit privileged accounts across the network, regardless of the platform or the CPM access. DNA can provide additional discovery functions, such as identifying machines vulnerable to Pass-the-Hash attacks, collecting reliable and comprehensive audit information, and generating reports and visual maps that evaluate the privileged account security status in the organization2. DNA can also be used before or independently of the CyberArk PAM solution, as it does not require agents to be installed on target systems2.
Reference: 1: Auto-detection
2: CyberArk DNA Overview

20.Which of the following files must be created or configured m order to run Password Upload Utility? Select all that apply.
A. PACli.ini
B. Vault.ini
C. conf.ini
D. A comma delimited upload file
Answer: A, C, D
Explanation:
: To run the Password Upload Utility, you need to create or configure the following files:
A comma delimited upload file: This is a text file that contains the passwords and their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line1.
PACli.ini: This is a configuration file that stores the parameters for the PACli, which is a command-line interface that enables communication between the Password Upload Utility and the Vault. The PACli.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: Vault, User, Password, and LogFile2.
conf.ini: This is a configuration file that stores the parameters for the Password Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile3.
You do not need to create or configure the following file to run the Password Upload Utility: Vault.ini: This is a configuration file that stores the parameters for the Vault server, such as the database name, port, and password. This file is not used by the Password Upload Utility, and it is not located in the same folder as the Password

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Upload Utility executable file. The Vault.ini file is located in the Vault installation folder, and it is used by the Vault service and the PrivateArk Client4.
Reference: 1: Create the Password File
2: PACli.ini
3: Password Upload Utility Parameter File (conf.ini)
4: [CyberArk Privileged Access Security Implementation Guide], Chapter 2: Installing the Vault,
Section: Configuring the Vault, Subsection: Vault.ini

21.Users can be resulted to using certain CyberArk interfaces (e.g.PVWA or PACLI).
A. TRUE
B. FALSE
Answer: A
Explanation:
Users can be restricted to using certain CyberArk interfaces (e.g. PVWA or PACLI) by using the User Type property. The User Type property is a parameter that can be configured in the User Management settings for each user. The User Type property defines which interfaces the user can access the Vault through, such as PVWA, PrivateArk Client, PACLI, PSM, etc. The User Type property is determined by the CyberArk license and can be assigned to users when they are added to the Vault or when their properties are updated. For example, if a user is assigned the User Type of EPVUser, they can access the Vault through PVWA, PrivateArk Client, PrivateArk Webclient, PACLI, and PIMSU. However, if a user is assigned the User Type of BizUser, they can only access the Vault through PVWA1. Therefore, by using the User Type property, administrators can control and restrict which CyberArk interfaces the users can use.
Reference: 1: Manage users, Types of users subsection

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

22.What is the purpose of the HeadStartInterval setting m a platform?
A. It determines how far in advance audit data is collected tor reports
B. It instructs the CPM to initiate the password change process X number of days before expiration.
C. It instructs the AIM Provider to ‘skip the cache' during the defined time period
D. It alerts users of upcoming password changes x number of days before expiration.
Answer: B
Explanation:
The purpose of the HeadStartInterval setting in a platform is to instruct the CPM to initiate the password change process X number of days before expiration. This setting is used when the platform has the One Time Password feature enabled, which means that the passwords are changed every time they are retrieved by a user. The HeadStartInterval setting defines the number of days before the password expires

(according to the ExpirationPeriod parameter) that the CPM will start the password change process. This gives the CPM enough time to change the password before it becomes invalid, and ensures that the user will always receive a valid password when they request it1. The HeadStartInterval setting can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 0, which means that the CPM will start the password change process on the same day as the password expiration date1. The other options are not the purpose of the HeadStartInterval setting in a platform:
A. It determines how far in advance audit data is collected for reports. This option is not related to the HeadStartInterval setting, which does not affect the audit data collection or reporting. The audit data is collected by the Vault server and stored in the Audit database, and the reports are generated by the PVWA or the PrivateArk Client based on the audit data2.
C. It instructs the AIM Provider to 'skip the cache' during the defined time period. This option is not related to the HeadStartInterval setting, which does not affect the AIM Provider or the cache mechanism. The AIM Provider is a component that enables applications to securely retrieve credentials from the Vault without requiring human intervention. The cache mechanism is a feature that allows the AIM Provider to store credentials locally for a limited time, in case of a temporary network failure or Vault unavailability3.
D. It alerts users of upcoming password changes x number of days before expiration. This option is not related to the HeadStartInterval setting, which does not alert users of anything. The HeadStartInterval setting only instructs the CPM to initiate the password change process, not to notify the users. The users do not need to be aware of the password changes, as they are performed automatically by the CPM and do not affect the user experience1.
Reference: 1: Privileged Account Management, Min Validity Period subsection
2: Reports and Audits
3: Application Identity Manager

Use CyberAM PAM-DEF Exam Questions to Pass Your Exam Smartly

23.It is possible to restrict the time of day, or day of week that a [b]reconcile[/b] process can occur
A. TRUE
B. FALSE
Answer: A
Explanation:
It is possible to restrict the time of day, or day of week that a reconcile process can occur by using the Reconcile Safe option in the Platform Management section of the PrivateArk Client. This option allows the administrator to define the reconcile schedule for each platform, which specifies when the reconcile process can run and how often it should be performed. The reconcile schedule can be set to run daily, weekly, monthly, or on specific days and times. By restricting the reconcile process, the

administrator can reduce the risk of unauthorized access to the accounts and improve the performance of the system.
Reference: [Defender PAM Course], Module 5: Reconcile and Rotate, Lesson 1: Reconcile and Rotate Overview,
Slide 9: Reconcile Safe
[Defender PAM Study Guide], Section 5.1: Reconcile and Rotate Overview, Page 24: Reconcile Safe [CyberArk Documentation], Privileged Access Security Implementation Guide, Chapter 5: Configure the Vault, Section 5.4: Configure Platforms, Subsection 5.4.2: Reconcile Safe

24.Which of the following options is not set in the Master Policy?
A. Password Expiration Time
B. Enabling and Disabling of the Connection Through the PSM
C. Password Complexity
D. The use of “One-Time-Passwords”
Answer: C
Explanation:
Password Complexity is not set in the Master Policy, but in the Platform Management settings for each platform. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. Password Complexity is a technical setting that defines the minimum requirements for the length and composition of the passwords that are generated by the CPM for the accounts associated with the platform2. Password Complexity can be configured in the Platform Management settings, which are independent of the Master Policy and can be customized according to the organization’s environment and security policies1.
The other options are set in the Master Policy, as follows:
A. Password Expiration Time: This is a policy rule that determines how often passwords are changed. It can be set in the Master Policy under the Password Management section1.
B. Enabling and Disabling of the Connection Through the PSM: This is a policy rule that determines whether users can connect to target systems through the PSM. It can be set in the Master Policy under the Session Management section1.
D. The use of “One-Time-Passwords”: This is a policy rule that determines whether passwords are changed every time they are retrieved by a user. It can be set in the Master Policy under the Password Management section1.
Reference: 1: The Master Policy
2: Platform Management, Password Complexity subsection

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

25.The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).
A. TRUE
B. FALSE
Answer: A
Explanation:
The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability). Exclusive accounts are accounts that can only be used by one user at a time, and are locked during usage. This means that no other user can access the same account until the current user releases it or the session expires. By using exclusive accounts, the organization can enforce individual accountability and traceability for the actions performed on the target systems. Exclusive accounts also reduce the risk of credential theft and unauthorized access, as the passwords are changed every time they are retrieved by a user1. Exclusive accounts can be configured in the Master Policy under the Password Management section, by enabling the Exclusive Access rule2.
Reference: 1: The Master Policy, One Time Password subsection
2: The Master Policy, Exclusive Access subsection

26.You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to [b]change [/b] the root account's password the CPM will…..
A. Log in to the system as root, then change root's password
B. Log in to the system as the logon account, then change roofs password
C. Log in to the system as the logon account, run the su command to log in as root, and then change
root's password.
D. None of these
Answer: C
Explanation:
When attempting to change the root account's password, the CPM will log in to the system as the logon account, run the su command to log in as root, and then change root's password. This is because the logon account is used to initiate sessions to machines that do not permit direct logon, such as Unix systems that restrict root access. When a logon account is associated with a privileged account, it will be used to log onto the remote machine and then elevate itself to the role of the privileged user. As different types of machines might have different logon prompts or elevation commands, the CPM can use the AutoLogonSequenceWithLogonAccount parameter to define the logon process and the elevation to the privileged account. This parameter contains regular expression prompts and responses that define the logon process and subsequent activities. The regular expressions can include dynamic values that the CPM reads from the account properties, user parameters, or client-specific parameters1.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

For example, the following is a possible AutoLogonSequenceWithLogonAccount parameter for a Unix platform:

```
AutoLogonSequenceWithLogonAccount=
login: {LogonUsername}
Password: {LogonPassword}
{LogonUsername}@.*\$ su -
Password: {LogonPassword}
root@.*# {ChangeCommand}
root@.*# exit
{LogonUsername}@.*\$ exit
```

Use CyberArk PAM-DEF Exam Questions to Pa

This parameter instructs the CPM to log in to the system as the logon account, enter the logon password, run the su - command to switch to the root user, enter the logon password again, run the change command to change the root password, exit the root session, and exit the logon session1.
The other options are not correct, as follows:
A. Log in to the system as root, then change root's password. This option is not possible, because the root account cannot be used for direct logon. The logon account is associated with the root account to enable the CPM to access the system and change the password1.
B. Log in to the system as the logon account, then change root's password. This option is not effective, because the logon account does not have the permission to change the root's password. The logon account needs to elevate itself to the root user by using the su command before changing the password1.
D. None of these. This option is not valid, because there is a correct answer among the choices.
Reference: 1: Logon Accounts for SSH and Telnet Connections

27.It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur
A. TRUE
B. FALSE

Answer: A
Explanation:
It is possible to restrict the time of day, or day of week that a verify process can occur by using the Verify Time Window parameter in the Platform Management page. This parameter allows the administrator to define a time window for each platform, during which the verify process can be performed. The verify process will not run outside of this time window, unless it is manually initiated by the administrator. This feature can help reduce the load on the target systems and the network during peak hours.
Reference: [Defender PAM Course], Module 4: Managing Accounts, Lesson 2: Account Verification, Slide 8: Verify Time Window
[Defender PAM Documentation], Version 12.3, Administration Guide, Chapter 4: Managing
Platforms, Section: Verify Time Window

Use Cybe-ARK PAM-DEF Exam Questions to Pass Your Exam Smartly

28.Which of the Following can be configured in the Master Poky? Choose all that apply.
A. Dual Control
B. One Time Passwords
C. Exclusive Passwords
D. Password Reconciliation
D. Ticketing Integration
F. Required Properties
G. Custom Connection Components H. Password Aging Rules
Answer: A, B, C, H
Explanation:
The Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. The Master Policy includes the following main concepts1: Basic policy rules: These rules allow the administrator to define specific aspects of privileged account management, such as privileged access workflows, password management, session monitoring and auditing.
Advanced policy rules: Some basic policy rules have related advanced settings that provide more granular control over the policy enforcement.
Exceptions: These are policy rules that differ from the overall Master Policy for a specific scope of accounts, such as accounts associated with a specific platform.
The Master Policy rules are divided into four sections2:
Privileged Access Workflows: These rules define how the organization manages access to privileged accounts, such as requiring dual control, one-time passwords, exclusive passwords, transparent connections, reason for access, etc.
Password Management: These rules determine how passwords are managed, such as requiring password change, password verification, password reconciliation,

ticketing integration, required properties, custom connection components, etc. Session Management: These rules determine whether or not privileged sessions are recorded and how they are monitored, such as requiring session isolation, session recording, session audit, etc. Audit: This rule determines how Safe audits are retained, such as specifying the audit retention period.
Based on the above information, the following options can be configured in the Master Policy:
A. Dual Control: This is a basic policy rule in the Privileged Access Workflows section that determines whether users need to get approval from authorized users before accessing a privileged account2.
B. One Time Passwords: This is a basic policy rule in the Privileged Access Workflows section that determines whether users can only use a password once before it is changed2.
C. Exclusive Passwords: This is a basic policy rule in the Privileged Access Workflows section that determines whether users need to check out a password and prevent other users from accessing it until it is checked in2.
H. Password Aging Rules: This is a basic policy rule in the Password Management section that determines how often passwords need to be changed2.
The following options cannot be configured in the Master Policy:
D. Password Reconciliation: This is not a policy rule, but a process that restores the password of a
privileged account to the value that is stored in the Vault, in case it is changed or out of sync3.
E. Ticketing Integration: This is not a policy rule, but a feature that enables the integration of the Vault with external ticketing systems, such as ServiceNow, Jira, etc.
F. Required Properties: This is not a policy rule, but a platform setting that determines which properties are mandatory for adding accounts to a platform.
G. Custom Connection Components: This is not a policy rule, but a platform setting that determines which connection components are used to connect to target systems, such as PVWA, PSM, PSMP, etc.
Reference: 1: The Master Policy
2: Master Policy Rules
3: Password Reconciliation
: Ticketing Integration
: Required Properties
: Custom Connection Components

Use CyberARK PAM-DEF Exam Questions to Pass Your Exam Smartly

29.If a password is changed manually on a server, bypassing the CPM, how would you configure the account so that the CPM could resume management automatically?
A. Configure the Provider to change the password to match the Vault's Password
B. Associate a reconcile account and configure the platform to reconcile automatically
C. Associate a logon account and configure the platform to reconcile automatically

D. Run the correct auto detection process to rediscover the password
Answer: B
Explanation:
A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the account that has been changed manually, the CPM can use the reconcile account to restore the password of the account to the value that is stored in the Vault, in case it is changed or out of sync. This process is called password reconciliation and it ensures that the passwords are synchronized and available for use. To configure the account so that the CPM can resume management automatically, the platform that the account belongs to must have the following parameters set1: RCAutomaticReconcileWhenUnsynched: This parameter determines whether passwords will be reconciled automatically after the CPM detects a password on a remote machine that is not synchronized with its corresponding password in the Vault. The acceptable values are Yes or No. RCReconcileReasons: This parameter determines the codes that represent the CPM plugin errors that will launch a reconciliation process. The acceptable values are plug-in return codes separated by a comma.
RCFromHour, RCToHour: These parameters determine the time frame in hours during which the CPM can reconcile passwords, either manually or automatically. The acceptable values are 0-23 or -1 for none.
RCExecutionDays: This parameter determines the days of the week when the CPM will reconcile passwords. The acceptable values are days of the week, separated by commas.
Reference: 1: Password Reconciliation

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

30.What is the maximum number of levels of authorization you can set up in Dual Control?
A. 1
B. 2
C. 3
D. 4
Answer: B
Explanation:
Dual Control is a feature that allows you to set up a workflow for approving access requests to sensitive accounts. You can configure up to two levels of authorization for each account, meaning that you need up to two different authorizers to approve the request before the user can access the account. The authorizers can be either users or groups, and they can have different approval methods, such as email, SMS, or CyberArk interface.
Reference: [Defender PAM] course, Module 5: Privileged Session Management, Lesson 5.2: Dual Control [Defender PAM Sample Items Study Guide], Question 31

31.As long as you are a member of the Vault Admins group you can grant any permission on any safe.
A. TRUE
B. FALSE
Answer: B
Explanation:
The Vault Admins group is a predefined group that is automatically created during the installation or upgrade of the Vault. This group has all possible permissions in the Vault, and can create and manage other users, groups, platforms, policies, safes, and accounts. However, this group is not automatically added to every safe in the Vault, but only to some system safes that are used for administrative purposes. Therefore, being a member of the Vault Admins group does not guarantee that you can grant any permission on any safe, unless you are also a member or an owner of that safe. To grant permissions on a safe, you need to have the Authorize safe members authorization on that safe, which allows you to add or remove users or groups as safe members, and assign or revoke their authorizations. Alternatively, you can use the Administrator user, which is a predefined user that is a member of the Vault Admins group, and has all possible permissions on any safe in the Vault.
Reference: Predefined users and groups
Safe member authorizations

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

32.In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX system.
What is the BEST way to allow CPM to manage root accounts.
A. Create a privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Reconcile account of the target server's root account.
B. Create a non-privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Logon account of the target server's root account.
C. Configure the Unix system to allow SSH logins.
D. Configure the CPM to allow SSH logins.
Answer: B
Explanation:
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon account

33.Which of the following statements are NOT true when enabling PSM recording for

a target Windows server? (Choose all that apply)
A. The PSM software must be instated on the target server
B. PSM must be enabled in the Master Policy (either directly, or through exception)
C. PSMConnect must be added as a local user on the target server
D. RDP must be enabled on the target server
Answer: A, C
Explanation:
The following statements are not true when enabling PSM recording for a target Windows server: A. The PSM software must be instated on the target server. This is not true, because the PSM software is installed on a dedicated server that acts as a proxy between the user and the target server. The PSM server intercepts the user's connection request, initiates the connection to the target server, and records the privileged session. The target server does not need to have the PSM software installed on it1.
C. PSMConnect must be added as a local user on the target server. This is not true, because PSMConnect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The target server does not need to have a local user named PSMConnect on it2. The following statements are true when enabling PSM recording for a target Windows server:
B. PSM must be enabled in the Master Policy (either directly, or through exception). This is true, because the Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. One of the rules in the Master Policy is the Session Isolation rule, which determines whether or not privileged sessions are isolated and recorded by PSM. This rule can be enabled either directly in the Master Policy, or through an exception for a specific scope of accounts3.
D. RDP must be enabled on the target server. This is true, because RDP is the protocol that is used by PSM to connect to Windows servers. The target server must have RDP enabled and configured properly to allow the PSM server to access it. The PSM server must also have the RDP client installed on it4.
Reference: 1: Privileged Session Manager
2: PSMConnect and PSMAdminConnect
3: Session Isolation
4: Configure RDP for PSM

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

34.The Password upload utility can be used to create safes.
A. TRUE
B. FALSE
Answer: A
Explanation:

The Password Upload utility can be used to create safes, as well as password objects, folders, and platforms. The Password Upload utility works with the CyberArk Password Vault to create password objects from a passwords list and store them in the Vault. This enables you to upload large numbers of passwords automatically and makes the Vault implementation process quicker and more automatic. The Password Upload utility initiates the Vault environment required to store passwords in the safe and start working with them. This includes creating new safes, adding the CPM user as a safe owner, and sharing the safe with the Password Vault Web Access1.
Reference: 1: Password Upload Utility

35.Which Cyber Are components or products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? Select all that apply.
A. Discovery and Audit (DMA)
B. Auto Detection (AD)
C. Export Vault Data (EVD)
D. On Demand Privileges Manager (OPM)
E. Accounts Discovery
Answer: A, B, E
Explanation:
Discovery and Audit (DMA), Auto Detection (AD), and Accounts Discovery are CyberArk components or products that can be used to discover Windows Services or Scheduled Tasks that use privileged accounts.
Discovery and Audit (DMA) is a tool that scans Windows servers and workstations to identify privileged accounts that are used by Windows Services or Scheduled Tasks. DMA can also generate reports on the usage and risks of these accounts.
Auto Detection (AD) is a feature of the CyberArk Privileged Account Security Solution that automatically detects and onboards privileged accounts that are used by Windows Services or Scheduled Tasks. AD can also monitor and rotate the passwords of these accounts.
Accounts Discovery is a feature of the CyberArk Privileged Account Security Solution that scans the network to discover privileged accounts on various platforms, including Windows. Accounts Discovery can also identify accounts that are used by Windows Services or Scheduled Tasks.
Reference: : Discovery and Audit (DMA) User Guide
: Auto Detection Implementation Guide
: Accounts Discovery Implementation Guide

36.A Reconcile Account can be specified in the Master Policy.
A. TRUE
B. FALSE
Answer: B

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Explanation:
A Reconcile Account is not specified in the Master Policy, but in the Platform settings. The Master Policy defines the general password management settings for all the accounts in the Vault, such as the frequency of password rotation and verification. The Platform settings define the specific password management settings for each type of target system, such as the password complexity and the Reconcile Account.
Reference: Defender PAM course, Module 2: Password Management, Lesson 2: Master Policy and Platforms, slide 8
Defender PAM course, Module 2: Password Management, Lesson 3: Reconcile and Logon Accounts, slide 2
Defender PAM Sample Items Study Guide, Question 37
CyberArk Privileged Access Security Documentation, Password Management - Master Policy CyberArk Privileged Access Security Documentation, Password Management - Platforms

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

37.In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?
A. True.
B. False. Because the user can also enter credentials manually using Secure Connect.
C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect.
D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials.
Answer: B
Explanation:
In order to connect to a target device through PSM, the account credentials used for the connection do not necessarily have to be stored in the vault. The user can also enter credentials manually using Secure Connect, which is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc. To use Secure Connect, the user needs to specify the target system address and the connection component ID in the URL, and then enter the credentials in the PSM login screen1.
The other options are not correct, because:
A. True. This is not correct, because as explained above, the user can also enter credentials manually using Secure Connect.
C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect. This is not correct, because PSM Connect is a predefined user that is created on the PSM server during the installation. This user is

used to establish the connection between the PSM server and the target server, and to run the PSM processes. The PSM Connect user is not used to log into the target device as the end user2.
D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials. This
is not correct, because this option is essentially the same as Secure Connect, which is the correct
answer.
Reference: 1: Secure Connect
2: PSMConnect and PSMAdminConnect

38.SAFE Authorizations may be granted to_____.
Select all that apply.
A. Vault Users
B. Vault Group
C. LDAP Users
D. LDAP Groups
Answer: A, B, C, D
Explanation:
SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory.
Reference: Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4 Defender PAM Sample Items Study Guide, Question 39, page 15
CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4:
Managing Safes, Section: Safe Authorizations, page 4-12

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

39.Secure Connect provides the following. Choose all that apply.
A. PSM connections to target devices that are not managed by CyberArk.
B. Session Recording
C. Real-time live session monitoring.
D. PSM connections from a terminal without the need to login to the PVWA
Answer: A, B, C
Explanation:
Secure Connect provides the following features:
A. PSM connections to target devices that are not managed by CyberArk. This is true,

because Secure Connect is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc1.

B. Session Recording. This is true, because Secure Connect sessions are recorded by PSM and stored in the Vault, just like regular PSM sessions. The recorded sessions can be viewed and audited by authorized users through the PVWA or the PSM web interface2.

C. Real-time live session monitoring. This is true, because Secure Connect sessions can be monitored in real-time by authorized users through the PSM web interface. The PSM web interface allows users to view the live session screen, send messages to the session user, pause or terminate the session, and take control of the session if needed3.

The following feature is not provided by Secure Connect:

D. PSM connections from a terminal without the need to login to the PVWA. This is false, because Secure Connect requires users to login to the PVWA and initiate the connection from there. The PVWA provides the URL for the Secure Connect session, which contains the target system address and the connection component ID. The user then needs to copy and paste the URL into a browser or a remote connection manager to launch the session1.

Reference: 1: Secure Connect

2: Recorded Sessions

3: PSM Web Interface

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

40.Which onboarding method would you use to integrate CyberArk with your accounts provisioning process?

A. Accounts Discovery

B. Auto Detection

C. Onboarding RestAPI functions

D. PTA Rules

Answer: C

Explanation:

The Onboarding RestAPI functions are a set of web services that allow you to integrate CyberArk with your accounts provisioning process. You can use the Onboarding RestAPI functions to create, update, delete, or verify accounts in the CyberArk Vault, as well as to retrieve information about accounts, platforms, and safes. The Onboarding RestAPI functions are part of the Central Credential Provider component, which is installed on a dedicated server that communicates with the Vault.

Reference: [Defender PAM Course], Module 4: Onboarding Accounts, Lesson:

41.What is the purpose of a linked account?
A. To ensure that a particular collection of accounts all have the same password.
B. To ensure a particular set of accounts all change at the same time.
C. To connect the CPNI to a target system.
D. To allow more than one account to work together as part of a password management process.
Answer: D
Explanation:
A linked account is an account that is associated with another account to enable the password management process. A linked account can be used for various purposes, such as logging on to a target system, changing the password of another account, or enabling privileged commands. A linked account can be defined either on the platform level or on the account level, depending on the type and scope of the linked account.
The types of linked accounts that are supported by CyberArk are1: Logon account: An account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the CPM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the CPM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account.
Reconcile account: An account that contains the password used in reconciliation processes. Reconciliation is a process that restores the password of a privileged account to the value that is stored in the Vault, in case it is changed or out of sync. A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the target account, the CPM can use the reconcile account to restore the password of the target account, in case it is changed or out of sync.
Other additional accounts: Additional accounts can be used in various cases. For example: Enable password: when managing network devices that require an enable password to access privileged mode.
Jump account: when using a custom plugin in a complex work flow that requires to first log on to a jump server.
The other options are not the purpose of a linked account, because:
A. To ensure that a particular collection of accounts all have the same password. This is not the purpose of a linked account, but of a group account. A group account is an account that is associated with multiple target systems that share the same credentials. A group account allows the CPM to manage the password of multiple systems with a single password object in the Vault2.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

B. To ensure a particular set of accounts all change at the same time. This is not the purpose of a linked account, but of a password change schedule. A password change schedule is a feature that allows the administrator to define a time frame for changing the passwords of a set of accounts. A password change schedule can be configured either in the Master Policy or in the Platform settings3.
C. To connect the CPNI to a target system. This is not the purpose of a linked account, but of a service account. A service account is an account that is used by a service or an application to connect to a target system. A service account can be managed by the Central Credential Provider (CCP),
which is a component that provides applications and services with the credentials they need to access target systems4.
Reference: 1: Linked Accounts
2: Group Accounts
3: Password Change Schedule
4: Service Accounts

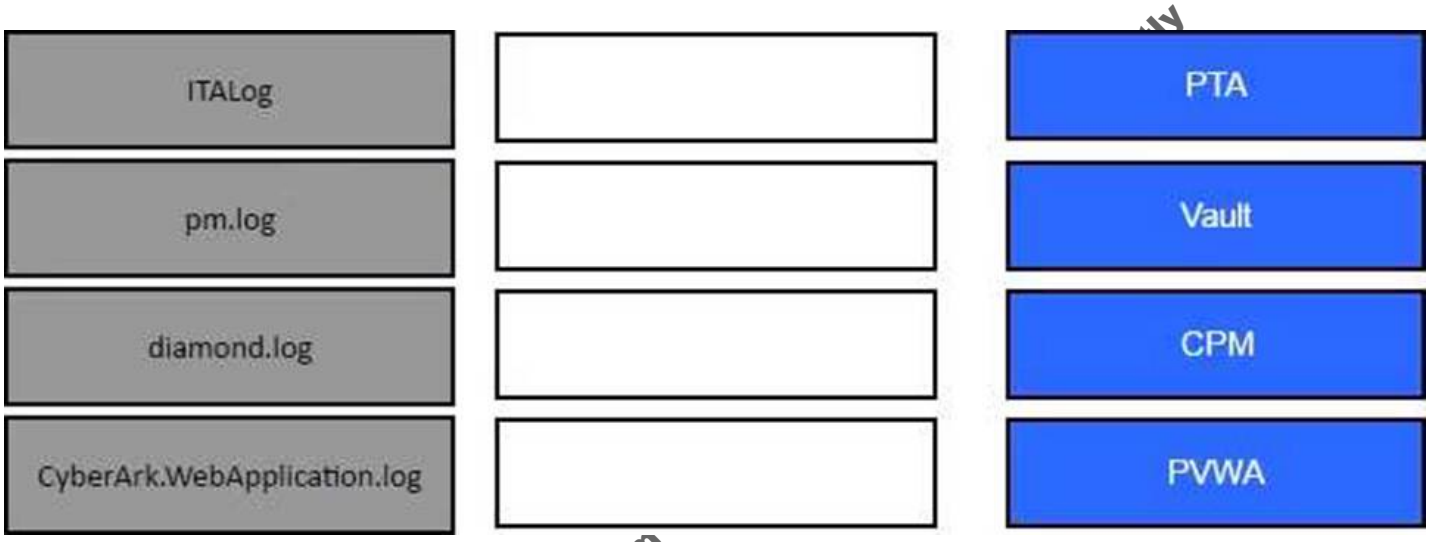
42.One can create exceptions to the Master Policy based on _____.
A. Safes
B. Platforms
C. Policies
D. Accounts
Answer: B
Explanation:
The Master Policy is a set of rules that apply to all accounts in the Vault. However, one can create exceptions to the Master Policy based on platforms, which are logical groupings of accounts that share common characteristics, such as operating system, device type, or application. By creating platform-specific policies, one can override the Master Policy settings for certain accounts and customize the security and management options for different platforms.
Reference: Defender PAM Sample Items Study Guide, page 9
CyberArk Core Privileged Access Security Documentation, Master Policy Overview and Platform-Specific Policies

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

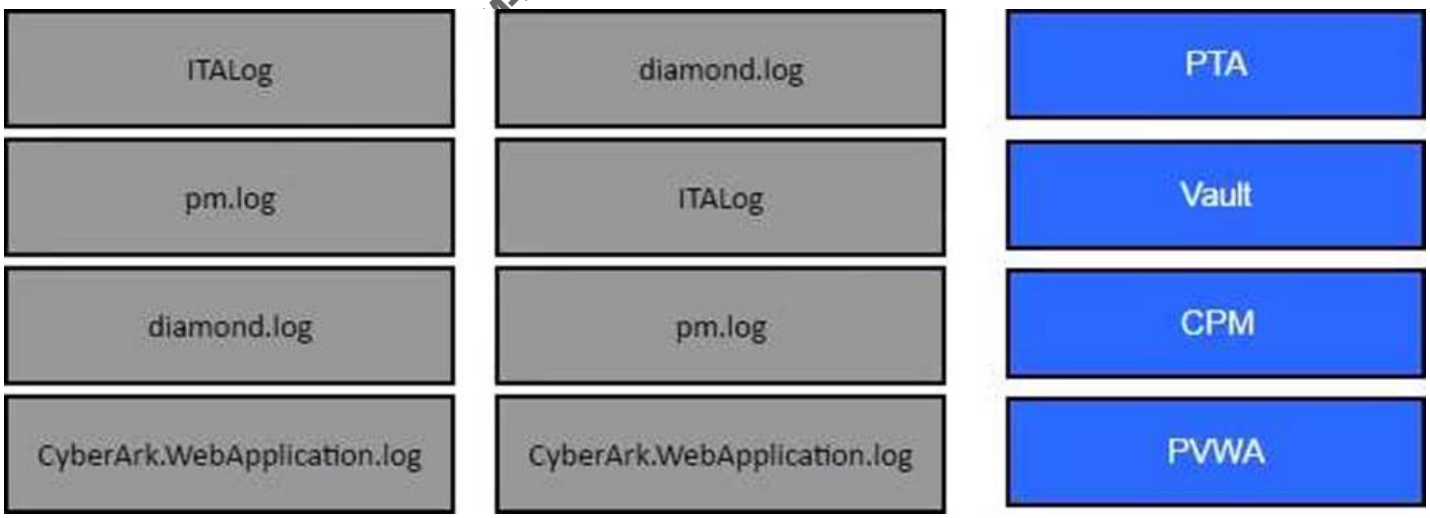
43.The vault supports Role Based Access Control.
A. TRUE
B. FALSE
Answer: A
Explanation:
The vault supports Role Based Access Control (RBAC), which is a method of granting access to resources based on the roles of users or groups. RBAC enables the

administrator to define roles that represent different functions or responsibilities in the organization, and assign permissions to those roles according to the principle of least privilege. Users or groups can then be assigned to one or more roles, and inherit the permissions of those roles. RBAC simplifies the management of access control by reducing the complexity and redundancy of assigning permissions to individual users or groups. RBAC also enhances security and compliance by ensuring that users or groups only have the minimum level of access required to perform their tasks1.
Reference: 1: Role Based Access Control

44.DRAG DROP
Match the log file name with the CyberArk Component that generates the log.



Answer:



Explanation:
Reference: Log Files
[Defender PAM Sample Items Study Guide], Question 46, page 16

45.Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?
A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.
C. Yes, if a logon account is associated with the root account.
D. No, it is not possible.
Answer: B
Explanation:
The ‘Connect’ button is a feature of the PVWA that allows users to initiate a privileged session to a target system through PSM without revealing the account credentials. The ‘Connect’ button can be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, but only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component. A logon account is a linked account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the PSM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the PSM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account. The PSM-SSH connection component is a predefined connection component that enables users to connect to Unix systems through PSM using SSH. The PSM-SSH connection component supports the use of logon accounts to access root accounts on Unix systems1.
The other options are not correct, because:
A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction. This is not correct, because PMTerminal.exe is a process that is used by the PSM-RDP connection component, not the PSM-SSH connection component. PMTerminal.exe is a terminal emulator that enables users to connect to Windows systems through PSM using RDP. PMTerminal.exe does not bypass the root SSH restriction, but rather uses the credentials stored in the Vault to authenticate to the target system2.
C. Yes, if a logon account is associated with the root account. This is not correct, because a logon account alone is not sufficient to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied. The user also needs to connect through the PSM-SSH connection component, which supports the use of logon accounts to access root accounts on Unix systems1. D. No, it is not possible. This is not correct, because it is possible to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, as explained in option B.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Reference: 1: Logon Accounts for SSH and Telnet Connections
2: Connect through PSM for SSH

46.A user with administrative privileges to the vault can only grant other users privileges that he himself has.
A. TRUE
B. FALSE
Answer: B
Explanation:
A user with administrative privileges to the vault can grant other users privileges that he himself
does not have, as long as he has the Authorize Users authorization on the Vault. The Authorize Users authorization enables a user to add or remove other users or groups as Vault members, and assign or revoke their authorizations. A user with this authorization can grant any privilege to any other user or group, regardless of his own privileges. However, this authorization does not allow a user to change his own privileges or the privileges of other users who have the same authorization1.
Reference: 1: Vault Member Authorizations

47.By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?
A. Vault Admins
B. Security Admins
C. Security Operators
D. Auditors
Answer: B
Explanation:
Security Admins are the built-in group that can view and configure Automatic Remediation and Session Analysis and Response in the PVWA. These features are part of the Privileged Threat Analytics (PTA) module, which is designed to detect and respond to anomalous activities and risky behaviors in the privileged environment. Security Admins have the permissions to access the PTA settings and configure the policies and actions for Automatic Remediation and Session Analysis and Response.
Reference: Defender PAM Sample Items Study Guide, page 18, question 49
Privileged Threat Analytics Implementation Guide, page 9, section “Security Admins”

48.CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.
A. TRUE
B. FALSE

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Answer: B
Explanation:
CyberArk does not implement license limits by controlling the number and types of users that can be provisioned in the vault. CyberArk implements license limits by controlling the number and types of users that can authenticate to the vault and use its features. The license limits are based on the user types and objects that are defined in the vault, such as Vault Users, LDAP Users, LDAP Groups, Safes, Accounts, etc. The license limits are enforced by the License Manager, which is a service that runs on the Vault server and monitors the license usage. The License Manager can send notifications and alerts when the license usage reaches certain thresholds, and can also block or allow access to the vault based on the license status1.
Reference: 1: Manage the CyberArk License

49.Assuming a safe has been configured to be accessible during certain hours of the day, a Vault Admin may still access that safe outside of those hours.
A. TRUE
B. FALSE
Answer: A
Explanation:
A Vault Admin may still access a safe outside of the hours that it has been configured to be accessible, as long as he has the Bypass Safe Time Restrictions authorization on the Vault. The Bypass Safe Time Restrictions authorization enables a user to access any safe in the Vault, regardless of the time restrictions that are defined for that safe. This authorization is useful for emergency situations or maintenance tasks that require access to safes outside of the normal working hours. By default, the Vault Admins group has this authorization, as well as other administrative authorizations on the Vault1.
Reference: 1: Vault Member Authorizations

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

50.The Accounts Feed contains:
A. Accounts that were discovered by CyberArk in the last 30 days
B. Accounts that were discovered by CyberArk that have not yet been onboarded
C. All accounts added to the vault in the last 30 days
D. All users added to CyberArk in the last 30 days
Answer: B
Explanation:
The Accounts Feed is a feature of the CyberArk Privileged Access Security Solution that enables the discovery and provisioning of privileged accounts in the environment. The Accounts Feed contains the accounts that were discovered by CyberArk that have not yet been onboarded to the Vault. These accounts are displayed in the

Pending Accounts page in the PVWA, where the user can view, analyze, and onboard them according to various criteria. The Accounts Feed helps the user to identify and manage the unmanaged privileged accounts that pose a security risk1. The other options are not correct, because:
A. Accounts that were discovered by CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain all the accounts that were discovered by CyberArk in the last 30 days, but only the ones that have not yet been onboarded. The accounts that were already onboarded to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
C. All accounts added to the vault in the last 30 days. This is not correct, because the Accounts Feed does not contain the accounts that were added to the Vault, but the ones that are waiting to be onboarded. The accounts that were added to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
D. All users added to CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain the users that were added to CyberArk, but the accounts that are waiting to be onboarded. The users that were added to CyberArk are not part of the Accounts Feed, but are displayed in the Users page in the PVWA1.
Reference: 1: Accounts Feed

51.PSM for Windows (previously known as “RDP Proxy”) supports connections to the following target systems
A. Windows
B. UNIX
C. Oracle
D. All of the above
Answer: D
Explanation:
PSM for Windows supports connections to various types of target systems, including Windows, UNIX, Oracle, and others. PSM for Windows uses different connection components to establish and manage the sessions, depending on the type and protocol of the target system. For example, PSM-RDP is used for Windows systems, PSM-SSH and PSM-Telnet are used for UNIX systems, PSM-Toad and PSM-SQLPlus are used for Oracle databases, and so on.
Reference: PSM for Windows
Connect through Privileged Session Manager for Windows Supported connection components

52.What is the primary purpose of One Time Passwords?
A. Reduced risk of credential theft
B. More frequent password changes
C. Non-repudiation (individual accountability)

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization.
Answer: A
Explanation:
One Time Passwords (OTPs) are passwords that are valid for only one use or a limited time period. The primary purpose of OTPs is to reduce the risk of credential theft, which is a common attack vector for hackers and malicious insiders. By using OTPs, the exposure of the credentials is minimized, and the attacker cannot reuse the stolen password to access the target system. OTPs also enhance the security of the authentication process, as they add an extra layer of verification to the user's identity. OTPs can be generated by various methods, such as SMS, email, hardware tokens, software tokens, etc1.
The other options are not the primary purpose of OTPs, because:
B. More frequent password changes. This is not the primary purpose of OTPs, but a consequence of using them. OTPs require more frequent password changes, as they expire after one use or a limited time period. However, this is not the main goal of using OTPs, but rather a means to achieve the goal of reducing the risk of credential theft.
C. Non-repudiation (individual accountability). This is not the primary purpose of OTPs, but a benefit of using them. Non-repudiation means that the user cannot deny performing an action or accessing a resource, as there is sufficient evidence to prove their identity and activity. OTPs can help achieve non-repudiation, as they are unique and personal to each user, and can be traced back to the user's device or account. However, this is not the main goal of using OTPs, but rather an advantage of using them.
D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization. This is not the primary purpose of OTPs, but a feature of using them. OTPs can help prevent unauthorized access to privileged accounts, as they require the user to have both the OTP and the regular password to access the target system. This means that no single actor can use the password without authorization, as they would need the cooperation of another actor who has the OTP. However, this is not the main goal of using OTPs, but rather a capability of using them.
Reference: 1: One-time password

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

53.Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.
A. TRUE
B. FALSE
Answer: B
Explanation:

Users who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The ‘Access Safe without confirmation’ safe permission is a special permission that allows a user to bypass the Dual control mechanism and access the accounts in the safe without requiring confirmation from other authorized users. This permission can be useful for emergency situations or trusted users who need immediate access to the accounts. However, this permission also increases the risk of unauthorized or malicious access, so it should be granted with caution and monitored closely1.
Reference: 1: Access without confirmation

54.Ad-Hoc Access (formerly Secure Connect) provides the following features. Choose all that apply.
A. PSM connections to target devices that are not managed by CyberArk.
B. Session Recording.
C. Real-time live session monitoring.
D. PSM connections from a terminal without the need to login to the PVWA.
Answer: A, B, C
Explanation:
Ad-Hoc Access (formerly Secure Connect) is a feature that allows users to connect to target devices that are not managed by CyberArk through the PSM. Users can specify the address, username, and password of the target device, and select a client to launch the connection. Ad-Hoc Access sessions benefit from the standard PSM features, such as session recording, detailed auditing, and real-time live session monitoring. However, Ad-Hoc Access does not allow users to connect from a terminal without logging in to the PVWA, as this would bypass the authentication and authorization mechanisms of CyberArk.
Reference: Configure ad hoc connections
Ad Hoc Connections
Privileged Remote Access Management C PAM Remote Access

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

55.When a group is granted the 'Authorize Account Requests' permission on a safe Dual Control requests must be approved by
A. Any one person from that group
B. Every person from that group
C. The number of persons specified by the Master Policy
D. That access cannot be granted to groups
Answer: C
Explanation:
When a group is granted the ‘Authorize Account Requests’ permission on a safe, dual control requests must be approved by the number of persons specified by the

Master Policy. This means that the request will be sent to all the members of the group, but only a certain number of them need to confirm it for the request to be authorized. The Master Policy defines the number of required approvers for each level of confirmation, as well as the number of levels. For example, if the Master Policy requires two approvers at the first level and one approver at the second level, then the request will be sent to the group and two members of the group must confirm it before it is sent to the second level of confirmation, where one more approver is needed.
Reference: Request access
Safe Members
CyberArk Defender - PAM Exam Practice Test

56.When managing SSH keys, the CPM stored the Private Key
A. In the Vault
B. On the target server
C.A&B
D. Nowhere because the private key can always be generated from the public key.
Answer: A
Explanation:
When managing SSH keys, the CPM stores the private key in the Vault. The CPM generates a new random SSH key pair and updates the public SSH key on the target server. The new private SSH key is then stored in the Digital Vault where it benefits from all the accessibility and security features of the Vault. The private SSH key is never stored on the target server, as this would expose it to unauthorized access or theft. The private SSH key cannot be generated from the public key, as this would defeat the purpose of asymmetric encryption.
Reference: Manage SSH Keys
SSH Key Manager
Use SSH Keys

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

57.When managing SSH keys, the CPM stores the Public Key
A. In the Vault
B. On the target server
C. A&B
D. Nowhere because the public key can always be generated from the private key.
Answer: B
Explanation:
When managing SSH keys, the CPM stores the public key on the target server. The CPM generates a new random SSH key pair and updates the public SSH key on the target machine. The public SSH key is stored in the home directory of the privileged user on the target machine, usually in the file ~/.ssh/authorized_keys. The public SSH

key is not stored in the Vault, as this would be redundant and unnecessary. The public SSH key cannot be generated from the private key, as this would defeat the purpose of asymmetric encryption.
Reference: Manage SSH Keys
SSH Key Manager
Use SSH Keys

58.Accounts Discovery allows secure connections to domain controllers.
A. TRUE
B. FALSE
Answer: B
Explanation:

59.Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed.
A. HeadStartInterval
B. Interval
C. ImmediateInterval
D. The CPM does not change the password under this circumstance
Answer: A
Explanation:

60.Vault admins must manually add the auditors' group to newly created safes so auditors will have sufficient access to run reports.
A. TRUE
B. FALSE
Answer: B
Explanation:
Vault admins do not need to manually add the auditors' group to newly created safes, because the auditors' group is automatically added to every safe in the vault by default. The auditors' group has the View Audit authorization, which allows its members to view the safe's activity and run reports.
However, vault admins can remove the auditors' group from specific safes if they want to restrict the access of the auditors.
Reference: Predefined users and groups - CyberArk

61.Which of the following Privileged Session Management solutions provide a detailed audit log of session activities?
A. PSM (i.e., launching connections by clicking on the "Connect" button in the PVWA)

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM SSH Proxy)
D. All of the above
Answer: D
Explanation:
All of the Privileged Session Management solutions provide a detailed audit log of session activities. PSM, PSM for Windows, and PSM for SSH enable organizations to secure, control and monitor privileged access to network devices by using Vaulting technology to manage privileged accounts and create detailed session audits and video recordings of all IT administrator privileged sessions on remote machines1. PSM also provides additional audit features such as SQL Command Level Audit, Windows Events Audit, and Universal Keystrokes Audit1. PSM for Web captures a detailed transcript of cloud application user activity to enable a security manager or auditor the ability to monitor sessions for suspicious or restricted operations2.
Reference: Monitor Privileged Sessions - CyberArk
Privileged Session Manager for Web - CyberArk

62.What is the primary purpose of Dual Control?
A. Reduced risk of credential theft
B. More frequent password changes
C. Non-repudiation (individual accountability)
D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization.
Answer: D
Explanation:
Dual control is a feature of CyberArk Defender PAM that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or ‘confirmation’ has been granted from an authorized Safe Owner (s). This is known as Dual Control. The primary purpose of dual control is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring confirmation from another authorized user, dual control ensures that there is a ‘collusion to commit’ fraud, meaning that at least two users are involved in the malicious activity and are accountable for it.
Reference: Dual Control - CyberArk
Dual Control - CyberArk
Dual control in V10 Interface - docs.cyberark.com

63.Time of day or day of week restrictions on when password verifications can occur

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

configured in _____.
A. The Master Policy
B. The Platform settings
C. The Safe settings
D. The Account Details
Answer: C
Explanation:
Time of day or day of week restrictions on when password verifications can occur are configured in the Safe settings. This is a security feature that prevents Safes from being opened except at certain times (e.g., 8 a.m. to 5 p.m.). If a user tries to enter at a time that has not been designated for access, they will receive a message that informs them that the Safe is unavailable.
Reference: Advanced Safe Management

64.Which parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests.
A. HeadStartInterval
B. Interval
C. ImmediateInterval
D. The CPM does not change the password under this circumstance
Answer: B
Explanation:
This parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests. It is set in the Master Policy under the Dual Control section. The value of this parameter determines the frequency of the CPM's verification process for accounts that have been accessed by users who have received confirmation from authorized Safe owners. The CPM will change the password of these accounts according to the value of this parameter.
Reference: Dual Control - CyberArk
Dual control in V10 Interface - docs.cyberark.com
PAM-DEF CyberArk Defender C PAM Questions and Answers - Marks4sure

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

65.According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?
A. PVWAUsers
B. Vault Admins
C. Auditors
D. PVWAMonitor
Answer: C
Explanation:
According to the CyberArk Defender-PAM study guide, the REPORTS page is used

to generate reports on various aspects of the CyberArk Privileged Access Management Solution, such as user activity, password usage, and compliance status. The default group that grants access to the REPORTS page is the Auditors group, which is a built-in group in the Vault that has the AuditUsers authorization. Members of the Auditors group can view and generate reports, but cannot modify them.
Reference: CyberArk Defender-PAM study guide, page 17, section 3.2.1
CyberArk Privileged Access Security Documentation, page 48, section 2.3.2.1

66.Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?
A. Require dual control password access Approval
B. Enforce check-in/check-out exclusive access
C. Enforce one-time password access
D. Enforce check-in/check-out exclusive access & enforce one-time password access
Answer: B
Explanation:
According to the CyberArk Defender PAM documentation, the Master Policy setting that must be
active in order to have an account checked-out by one user for a pre-determined amount of time is Enforce check-in/check-out exclusive access. This setting enables organizations to permit users to check out a 'one-time' password and lock it so that no other users can retrieve it at the same time. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account.
Reference: Account check-out and check-in - CyberArk
Master Policy - CyberArk

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

67.The password upload utility must run from the CPM server
A. TRUE
B. FALSE
Answer: A
Explanation:
According to the CyberArk documentation1, the Password Upload utility must run from the Central Policy Manager (CPM) server. This utility works by uploading passwords and their properties into the Password Vault from a pre-prepared file, creating the required environment, when necessary. It is run from a command line whenever a password upload is required1.

68.For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.
A. TRUE
B. FALSE
Answer: B
Explanation:
According to the CyberArk documentation1, once Object Level Access Control is enabled for a Safe, it cannot be disabled. This feature allows granular control over user access to passwords and files in the Safe, regardless of their Safe level member authorizations2. To enable Object Level Access Control, users need to have the Manage Safe authorization in the Vault1.

69.The vault supports Subnet Based Access Control.
A. TRUE
B. FALSE
Answer: A
Explanation:
According to the web page in the edge browser, the vault supports Subnet Based Access Control. This is a feature that allows you to restrict access to a key vault to a specified virtual network and subnet. You can also use firewall settings to deny internet traffic and allow only specific IP addresses. This way, you can enhance the security and privacy of your key vault data12

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

70.When creating an onboarding rule, it will be executed upon .
A. All accounts in the pending accounts list
B. Any future accounts discovered by a discovery process
C. Both “All accounts in the pending accounts list” and “Any future accounts discovered by a discovery process”
Answer: C
Explanation:
According to the CyberArk Defender PAM documentation1, when creating an onboarding rule, it will be executed upon both all accounts in the pending accounts list and any future accounts discovered by a discovery process. This means that the rule will automatically onboard and provision the accounts that match the rule criteria, regardless of when they were discovered. The rule will also apply to any new accounts that are discovered by subsequent discovery processes. This way, the onboarding rule can minimize the time and effort required to securely manage the accounts in the vault.

71.How does the Vault administrator apply a new license file?

A. Upload the license.xml file to the system Safe and restart the PrivateArk Server service
B. Upload the license.xml file to the system Safe
C. Upload the license.xml file to the Vault Internal Safe and restart the PrivateArk Server service
D. Upload the license.xml file to the Vault Internal Safe
Answer: C
Explanation:
According to the CyberArk Defender PAM documentation1, the Vault administrator can apply a new license file by uploading the license.xml file to the Vault Internal Safe and restarting the PrivateArk Server service. The Vault Internal Safe is a special Safe that contains the Vault configuration files, including the license file. The Vault administrator can access this Safe from the PrivateArk Client and replace the existing license file with the new one. After that, the Vault administrator must restart the PrivateArk Server service for the changes to take effect. This procedure can be done either from the Vault machine or from a remote machine.
Reference: Manage the CyberArk License - CyberArk

72.When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy).
A. True
B. False, a user can submit the request after the connection has already been initiated via the PSM for Windows
Answer: A
Explanation:
According to the CyberArk Defender PAM documentation1, when Dual Control is enabled, a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy). This is a security feature that ensures that passwords can only be retrieved after permission or ‘confirmation’ has been granted from an authorized Safe Owner(s). The user must specify the reason for accessing the account, whether they will access it once or multiple times, and the time period during which they will access it. The request is then sent to the authorized Safe Owners, who can either confirm or reject it. The number of confirmations required is defined in the Master Policy. Only after the user receives the required confirmations, they can activate the request and access the account through PSM for Windows. This way, Dual Control adds an additional measure of protection and accountability for accessing sensitive accounts.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

73.Which of the following PTA detections require the deployment of a Network Sensor

or installing the PTA Agent on the domain controller?
A. Suspected credential theft
B. Over-Pass-The-Hash
C. Golden Ticket
D. Unmanaged privileged access
Answer: C
Explanation:
According to the CyberArk Defender PAM documentation1, the PTA detection that requires the deployment of a Network Sensor or installing the PTA Agent on the domain controller is Golden Ticket. A Golden Ticket is a type of attack that involves creating a forged Kerberos Ticket Granting Ticket (TGT) that grants the attacker access to any resource in the domain. The attacker needs to compromise the domain controller and steal the KRBTGT account password hash to create the Golden Ticket. The PTA Network Sensor or the PTA Agent can detect this attack by analyzing the network traffic and identifying anomalies in the Kerberos protocol, such as TGTs with abnormal lifetime, encryption type, or renewal time. The PTA Server then alerts the security team and provides details about the attack, such as the source IP, the target domain, and the ticket properties.
Reference: PTA Network Sensors - CyberArk

74.Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client's machine makes an RDP connection to the PSM server, which user will be utilized?
A. Credentials stored in the Vault for the target machine
B. Shadowuser
C. PSMConnect
D. PSMAdminConnect
Answer: C
Explanation:
According to the CyberArk Defender PAM documentation1, when a user initiates a PSM connection to the target Linux machine using RemoteApp via PVWA, the client's machine makes an RDP connection to the PSM server using the PSMConnect user. The PSMConnect user is a local or domain user that starts PSM sessions on the PSM machine. The PSMConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMConnect user retrieves the credentials of the target account from the vault and uses them to establish a
secure connection to the target machine. The user can then interact with the target machine through the PSM session, while the PSM server records and audits the session activity.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

75.Which report shows the accounts that are accessible to each user?
A. Activity report
B. Entitlement report
C. Privileged Accounts Compliance Status report
D. Applications Inventory report
Answer: B
Explanation:
The report that shows the accounts that are accessible to each user is the Entitlement report. According to the web page in the edge browser, the Entitlement report provides information about users' entitlement rights in PAM - Self-Hosted regarding user, Safe, active platform, target machine, target account, etc. This report includes each user's effective access control and authorization level on each account that the user has access to in PAM - Self-Hosted. The Entitlement report can be generated in PVWA or PrivateArk1.

76.The Vault administrator can change the Vault license by uploading the new license to the system Safe.
A. True
B. False
Answer: A
Explanation:
According to the web search results, the Vault administrator can change the Vault license by uploading the new license to the system Safe123. This can be done either from the Vault machine or from a remote machine using the PrivateArk client. The new license file should be named license.xml and replace the current one in the system Safe. This can be done without having to reinstall the Vault or restart the service.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

77.A Vault administrator have associated a logon account to one of their Unix root accounts in the vault.
When attempting to verify the root account's password the Central Policy Manager (CPM) will:
A. ignore the logon account and attempt to log in as root
B. prompt the end user with a dialog box asking for the login account to use
C. log in first with the logon account, then run the SU command to log in as root using the password in the Vault
D. none of these
Answer: C
Explanation:
According to the web search results, when a Vault administrator has associated a logon account to one of their Unix root accounts in the vault, the CPM will log in first

with the logon account, then run the SU command to log in as root using the password in the Vault1. This is a common use case for using a logon account, as the best practice for Unix systems is to disallow the root user from logging in using SSH, which is what the CPM uses to sign in to a system to manage the password2. The logon account can be defined on the target account level or on the platform level, making it available to all accounts associated with the platform2. The CPM can also use the logon account to initiate PSM sessions to the target machine3.

78.Which is the primary purpose of exclusive accounts?
A. Reduced risk of credential theft
B. More frequent password changes
C. Non-repudiation (individual accountability)
D. To force a ‘collusion to commit’ fraud ensuring no single actor may use a password without authorization
Answer: D
Explanation:
According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables organizations to permit users to check out a ‘one-time’ password and lock it so that no other users can retrieve it at the same time1. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account1.
The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a ‘collusion to commit’ fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

79.What is the chief benefit of PSM?
A. Privileged session isolation
B. Automatic password management
C. Privileged session recording
D. ‘Privileged session isolation’ and ‘Privileged session recording’
Answer: D
Explanation:
According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session

isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user's activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

80.A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.
A. True
B. False
Answer: A
Explanation:
According to the web search results, a Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control. SMTP is a protocol that enables the sending and receiving of email messages. By integrating SMTP with CyberArk Defender PAM, the Event Notification Engine (ENE) can automatically send email notifications about PAM activities to predefined users1. For example, the ENE can notify users about password requests, password confirmations, password changes, password verifications, password
reconciliations, password access, password usage, password expiration, and password
violations1. The ENE can also notify users about system events, such as Vault backup, Vault restore, Vault shutdown, Vault startup, and Vault license expiration1. These notifications help to monitor the Vault activity and ensure compliance with the security policies.
SMTP integration is also essential for facilitating workflow processes, such as Dual Control. Dual Control is a feature that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner(s). This is known as Dual Control2. SMTP integration enables the ENE to send email notifications to the requesters and the confirmers about the status of the password requests. The ENE can also send reminders to the confirmers if they have not responded to the requests within a specified time period2. These notifications help to streamline the workflow process and ensure timely and secure access to the accounts.
Reference: Email notifications - CyberArk

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

81.CyberArk recommends implementing object level access control on all Safes.
A. True
B. False
Answer: B
Explanation:
CyberArk does not recommend implementing object level access control on all Safes. According to the CyberArk documentation1, enabling object level access control impacts Vault performance. Therefore, it should be used only when necessary and with caution. Object level access control is useful when you need to give granular permissions to specific passwords or files in a Safe, regardless of the Safe level member authorizations. For example, you can use it to grant access to an external vendor or technician for a specific password only, without exposing any other passwords or files in the Safe. However, if you do not need this level of granularity, you can use the regular Safe member authorizations to control user access to the Safe and its contents.

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

82.Which of the following logs contains information about errors related to PTA?
A. ITAlog.log
B. diamond.log
C. pm_error.log
D. WebApplication.log
Answer: B
Explanation:
According to the web search results, the diamond.log is the main log file that records the PTA system activities, such as receiving and processing events, generating alerts, and sending notifications1. The diamond.log also contains information about errors related to PTA, such as connection failures, configuration issues, parsing problems, or internal exceptions2. The diamond.log can be found in the /opt/tomcat/logs directory on the PTA machine1. The debug level of the diamond.log can be changed using the changeLogLevel.sh utility or manually editing the log4j.properties file1. The diamond.log can be used for troubleshooting PTA issues and viewing statistics

83.An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor’s machine makes an RDP connection the PSM server, which user will be used?
A. PSMAdminConnect
B. Shadowuser
C. PSMConnect

D. Credentials stored in the Vault for the target machine
Answer: A
Explanation:
According to the web search results, when an auditor initiates a live monitoring session to PSM server to view an ongoing live session, the auditor's machine makes an RDP connection to the PSM server using the PSMAdminConnect user. The PSMAdminConnect user is a local or domain user that starts PSM sessions on the PSM machine for authorized users who want to monitor or terminate active sessions1. The PSMAdminConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMAdminConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The auditor can then view the live session through the PSM session, while the PSM server records and audits the session activity.

84.Which keys are required to be present in order to start the PrivateArk Server service?
A. Recovery public key
B. Recovery private key
C. Server key
D. Safe key
Answer: A, C
Explanation:
The server key and the public recovery key are required to be present in order to start the PrivateArk Server service. The server key opens the Vault, much like the key of a physical Vault. The public recovery key is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. The server key and the public recovery key are usually stored on a removable media, such as a disk or CD, so that they can be safely secured in a physical safe. The recovery private key and the safe key are not needed to start the PrivateArk Server service. The recovery private key is only used for recovery purposes and the safe key is only used to access a specific safe that is defined with an external key.
Reference: Server keys, Server Components

85.Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?
A. PSM (i.e., launching connections by clicking on the connect button in the Password Vault Web Access (PVWA)
B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM-SSH Proxy)
D. All of the above

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Answer: D
Explanation:
According to the web search results, all of the Privileged Session Management (PSM) solutions support live monitoring of active sessions. PSM, PSM for Windows, and PSM for SSH enable authorized users to monitor active sessions from their workstation and take part in controlling these sessions. Users can also suspend or terminate active sessions based on their group assignment. By default, active session monitoring is enabled at system level for all authorized users, and can be disabled at platform level. Active session monitoring can also be disabled at system level, but when it is disabled, it cannot be enabled at platform level. PSM can automatically suspend or terminate sessions when notified by PTA or a third party threat analytics tool1. Authorized users monitor or terminate an active session using the same connection method (RDP file or HTML5 Gateway) as the end user

86.Within the Vault each password is encrypted by:
A. the server key
B. the recovery public key
C. the recovery private key
D. its own unique key
Answer: D
Explanation:
According to the web search results, within the Vault each password is encrypted by its own unique key. This key is generated by the Vault when the password is added to the Vault and is stored in the Vault's database. The password key is encrypted by the safe key, which is the key of the safe that contains the password. The safe key is encrypted by the server key, which is the key that opens the Vault. The server key is encrypted by the public recovery key, which is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. This layered encryption scheme ensures that each password is protected by multiple keys and that no single key can compromise the security of the Vault

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

87.When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.
A. True; this is the default behavior
B. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file
C. True, if the AllowFailback setting is set to "yes" in the padr.ini file
D. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the dbparm.ini file
Answer: B
Explanation:

According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online. The Vault administrator must manually set the DR Vault to DR mode by setting “FailoverMode=no” in the padr.ini file1. This file is located in the /opt/CARKaim/conf directory on the DR Vault machine2. The Vault administrator must also stop the replication process on the DR Vault and restart the PrivateArk Server service1. This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover1. The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario3. The dbparm.ini file is not relevant for the DR
failback process, as it contains the database parameters for the Vault server.
Reference: Initiate a DR failback to the Production Vault - CyberArk
Install the Disaster Recovery application - CyberArk
Cascading DR - CyberArk
[dbparm.ini file - CyberArk]

88.Which user(s) can access all passwords in the Vault?
A. Administrator
B. Any member of Vault administrators
C. Any member of auditors
D. Master
Answer: D
Explanation:
According to the CyberArk Defender PAM documentation1, the Master user is the only user that can access all passwords in the Vault. The Master user is a special user that is created during the initial installation of the Vault and has full permissions on all Safes and accounts in the Vault. The Master user can also perform administrative tasks, such as backup and restore the Vault, change the Vault license, and manage the recovery key. The Master user is the only user that can log on to the Vault in case of a disaster using the recovery key. The Master user’s password is not stored in the Vault and cannot be changed or retrieved by any other user.
The Administrator user is a predefined user that is created during the initial installation of the Vault and has the Vault Admin authorization. The Administrator user can perform administrative tasks, such as create and manage users and groups, define platforms and policies, and monitor Vault activity. However, the Administrator user cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2.
The Vault administrators group is a predefined group that is created during the initial installation of the Vault and has the Vault Admin authorization. The members of the Vault administrators group can perform the same administrative tasks as the Administrator user, but they cannot access any passwords in the Vault unless they

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

are explicitly added as a member of a Safe that contains the passwords2.
The auditors group is a predefined group that is created during the initial installation of the Vault and has the Audit Users authorization. The members of the auditors group can view and generate reports on the Vault activity, but they cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2.
Reference: Master User - CyberArk
Predefined users and groups - CyberArk

89.Which report could show all accounts that are past their expiration dates?
A. Privileged Account Compliance Status report
B. Activity log
C. Privileged Account Inventory report
D. Application Inventory report
Answer: A
Explanation:
The Privileged Account Compliance Status report shows the compliance status of all privileged accounts in the Vault, based on the expiration date and password change policy. This report can help identify accounts that are past their expiration dates and need to be updated or removed.
Reference: [Defender PAM Sample Items Study Guide], page 18, question 90
[CyberArk Privileged Access Security Documentation], version 12.3, Reports Guide, page 27, Privileged Account Compliance Status report

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

90.Which values are acceptable in the address field of an Account?
A. It must be a Fully Qualified Domain Name (FQDN)
B. It must be an IP address
C. It must be NetBIOS name
D. Any name that is resolvable on the Central Policy Manager (CPM) server is acceptable
Answer: D
Explanation:
The address field of an Account is used to identify the target system where the Account is located. The CPM uses this address to connect to the target system and perform password management operations. Therefore, the address field can be any name that is resolvable on the CPM server, such as a FQDN, an IP address, a NetBIOS name, or a custom name defined in the hosts file of the CPM server.
Reference: Defender PAM Sample Items Study Guide, page 9, question 91
CyberArk Privileged Access Security Implementation Guide, page 75, section “Address”

91.tsparm.ini is the main configuration file for the Vault.
A. True
B. False
Answer: B
Explanation:
tsparm.ini is not the main configuration file for the Vault. It is one of the several configuration files that control the initial settings and method of operation of the Server. The main configuration file for the Vault is DBParm.ini, which contains the general parameters of the database, such as the Vault name, the Vault IP address, the Vault port, the encryption algorithm, the log retention, and the debug mode.
Reference: Defender PAM Sample Items Study Guide, page 9, question 92
CyberArk Privileged Access Security Implementation Guide, page 75, section "DBParm.ini" CyberArk Vault Server Parameter Files, page 1, section "TSParm.ini"

92.Which combination of Safe member permissions will allow end users to log in to a remote machine transparently but NOT show or copy the password?
A. Use Accounts, Retrieve Accounts, List Accounts
B. Use Accounts, List Accounts
C. Use Accounts
D. List Accounts, Retrieve Accounts
Answer: B
Explanation:
The Use Accounts permission enables Safe members to log in to a remote machine through a PSM connection from the Accounts List or the Account Details page. The List Accounts permission enables Safe members to view the Accounts list. However, to show or copy the password, the Safe members also need the Retrieve Accounts permission, which allows them to view and copy the account value in the Account Details page or the Accounts list. Therefore, the combination of Use Accounts and List Accounts will allow end users to log in to a remote machine transparently but not show or copy the password.
Reference: Safe Members - CyberArk1, section "Permissions"
Safes and Safe members - CyberArk2, section "Safe members overview"

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

93.A logon account can be specified in the platform settings.
A. True
B. False
Answer: A
Explanation:
A logon account can be specified in the platform settings of CyberArk, a security software that manages privileged accounts and credentials. According to the

CyberArk documentation1, "In the Account Details window, in the CPM pane, in the accounts section, you can associate either a logon account or a reconciliation account. If a default logon account has been configured for the platform that manages this account, that account is listed. You can associate another logon account or leave the default account as it is."1 A logon account is an account that is used to log on to a target system and perform password management operations on other accounts. A reconciliation account is an account that is used to restore access to a target system when the logon account fails.

94.Which type of automatic remediation can be performed by the PTA in case of a suspected credential theft security event?
A. Password change
B. Password reconciliation
C. Session suspension
D. Session termination
Answer: A
Explanation:
The PTA can perform automatic password change as a type of remediation in case of a suspected credential theft security event. According to the CyberArk documentation1, "Rotate credentials - for OverPass the Hash attack and Suspected credentials theft events."1 This means that the PTA can initiate a password change request to the CPM for the affected account, which will generate a new random password and update it on the target system and the Vault. This way, the PTA can prevent the attacker from using the stolen credentials to access the target system or launch further attacks.
Reference: Configure PTA Remediations - CyberArk, section “Remediation Initiation”

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

95.dbparm.ini is the main configuration file for the Vault.
A. True
B. False
Answer: B
Explanation:
dbparm.ini is not the main configuration file for the Vault. It is one of the several configuration files
that control the initial settings and method of operation of the Server. The main configuration file for
the Vault is DBParm.ini, which contains the general parameters of the database, such as the Vault
name, the Vault IP address, the Vault port, the encryption algorithm, the log retention, and the
debug mode1.

Reference: DBParm.ini - CyberArk, section “Main parameters”

96.A user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings.
What is the issue?
A. The user must login as PSMAdminConnect
B. The PSM service is not running
C. The user is not a member of the PVWAMonitor group
D. The user is not a member of the Auditors group
Answer: D
Explanation:
To access the Monitoring tab and view the recordings of the PSM sessions, the user must have membership in the Auditors group or membership in the relevant Account Safes and Recording Safes with the appropriate permissions1. The user must also use the same connection method (RDP file or HTML5 Gateway) as the end user who conducted the session1. The other options are not relevant to the issue, as the user does not need to login as PSMAdminConnect, the PSM service is running if the user was able to conduct a session, and the PVWAMonitor group is not a valid group in CyberArk.
Reference: Monitor Privileged Sessions - CyberArk, section “The MONITORING page”

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

97.Which of the following components can be used to create a tape backup of the Vault?
A. Disaster Recovery
B. Distributed Vaults
C. Replicate
D. High Availability
Answer: C
Explanation:
The Replicate component can be used to create a tape backup of the Vault. The Replicate component is a utility that exports the encrypted contents of the Safes and the Vault metadata to a computer outside the Vault environment. A global backup system can then access the replicated files and copy them to a tape or any other backup media. The Replicate component is part of the CyberArk Backup Process, which provides a secure and easy method of backing up and restoring the Vault data12. The other components are not related to the tape backup of the Vault. Disaster Recovery is a feature that enables the Vault to recover from a catastrophic failure by using a standby Vault server3. Distributed Vaults is a feature that enables the Vault to synchronize data with other Vaults in different locations4. High Availability is a feature that enables the Vault to maintain continuous operation by using a

primary and a secondary Vault server.
Reference: Use the CyberArk Backup Process - CyberArk, section “Use the CyberArk Backup Process” Install the Vault Backup Utility - CyberArk, section “Backup utilities” Disaster Recovery - CyberArk, section “Disaster Recovery” Distributed Vaults - CyberArk, section “Distributed Vaults” [High Availability - CyberArk], section “High Availability”

98.Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)
A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed
B. Copy the entire contents of the CD to the system Safe on the Vault
C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions
D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions
Answer: A, B, D
Explanation:
A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed. This option ensures that the CD is kept in a secure location when not in use, and that the keys are available when needed. This is the default option suggested by CyberArk1.
B. Copy the entire contents of the CD to the system Safe on the Vault. This option allows the Vault to access the keys from the system Safe, which is a special Safe that stores the Vault configuration files and keys. The system Safe is encrypted and protected by the Vault, and can only be accessed by authorized users2.
D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD
to a folder on the Vault Server and secure it with NTFS permissions. This option provides an additional layer of security for the server key, which is the most critical key for the Vault. An HSM is a physical device that stores and manages cryptographic keys in a tamper-resistant and isolated environment. The Vault can integrate with an HSM to store and retrieve the server key3. The rest of the keys can be stored in a folder on the Vault Server and secured with NTFS permissions, which restrict access to authorized users and groups.
The following option is not secure and should be avoided:
C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions. This option exposes the keys to potential risks, such as unauthorized access, data corruption, or deletion. NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. Moreover, this option does not comply with the CyberArk best practices, which recommend to store the keys on a

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

removable media or an HSM

99.Which of these accounts onboarding methods is considered proactive?
A. Accounts Discovery
B. Detecting accounts with PTA
C. A Rest API integration with account provisioning software
D. A DNA scan
Answer: C
Explanation:
A Rest API integration with account provisioning software is considered a proactive account onboarding method, because it enables the automatic creation and management of accounts in the Vault as soon as they are provisioned in the target systems. This way, the accounts are secured from the start and do not need to be discovered or onboarded manually later. A Rest API integration with account provisioning software can be achieved by using the CyberArk Accounts Feed REST API, which allows external applications to send account information to the Vault1.
The other options are not proactive account onboarding methods, because they rely on the discovery
of existing accounts that may have been exposed or compromised before being onboarded to the
Vault. Accounts Discovery is a feature that enables the Vault to scan target systems and identify
privileged accounts that are not managed by the Vault2. Detecting accounts with PTA is a feature that
enables the Privileged Threat Analytics (PTA) component to detect and alert on suspicious account
activities and credential theft3. A DNA scan is a feature that enables the Discovery and Audit (DNA)
tool to scan Windows and Unix machines and generate a report on the privileged accounts and
vulnerabilities found4.
Reference: CyberArk Accounts Feed REST API - CyberArk, section “CyberArk Accounts Feed REST API” Accounts Discovery - CyberArk, section “Accounts Discovery”
Detect and Respond to Privileged Account Threats - CyberArk, section “Detect and Respond to Privileged Account Threats”
CyberArk DNA - CyberArk, section “CyberArk DNA”

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

100.When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online.
A. True; this is the default behavior

B. False; this is not possible
C. True, if the AllowFailback setting is set to “yes” in the padr.ini file
D. True, if the AllowFailback setting is set to “yes” in the dbparm.ini file
Answer: C
Explanation:
When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online, if the AllowFailback setting is set to “yes” in the padr.ini file. The padr.ini file is the configuration file for the Disaster Recovery application, which enables the DR Vault to replicate data from the Primary Vault and take over its role in case of a failure. The AllowFailback setting determines whether the DR Vault will automatically switch back to the passive mode when the Primary Vault is restored. The default value of this setting is “no”, which means that the DR Vault will remain active until a manual failback is performed1. To enable the automatic failback, the setting must be changed to “yes” and the padr service must be restarted1. The dbparm.ini file is not relevant to this setting, as it is the main configuration file for the Vault database2.
Reference: Configure the DR Vault - CyberArk, section “AllowFailback” DBParm.ini - CyberArk, section “Main parameters”

Use CyberArk PAM-DEF Exam Questions to Pass Your Exam Smartly

Get full version of
PAM-DEF Q&As